FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 17-97; FCC 24-120; FR ID 304848]

Call Authentication Trust Anchor

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) adopts rules that strengthen the Commission's caller ID authentication requirements by establishing clear practices for providers that rely on third parties to fulfill their STIR/SHAKEN implementation obligations. The rules authorize providers with a STIR/SHAKEN implementation obligation to engage third parties to perform the technological act of digitally "signing" calls consistent with the requirements of the STIR/SHAKEN technical standards so long as: the provider with the implementation obligation makes the "attestation-level" decisions for authenticating caller ID information; and all calls are signed using the certificate of the provider with the implementation obligation—not the certificate of a third party. The rules also explicitly require all providers with a STIR/SHAKEN implementation obligation to obtain a Service Provider Code (SPC) token from the STIR/SHAKEN Policy Administrator and present that token to a STIR/SHAKEN Certificate Authority to obtain a digital certificate. Additionally, the rules include recordkeeping requirements for third-party authentication arrangements to enable the Commission to monitor compliance with and enforce Commission rules.

DATES: These rules are effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

FOR FURTHER INFORMATION CONTACT: For further information about the *Notice of Proposed Rulemaking*, contact Emily Caditz, Attorney Advisor, Competition Policy Division, Wireline Competition Bureau, at Emily.Caditz@fcc.gov. For additional information concerning the Paperwork Reduction Act proposed information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele at (202) 418-2991.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order in WC Docket No. 17-97, FCC 24-120, adopted on November 21, 2024 and released on November 22, 2024. The complete text of this document is available for download at https://docs.fcc.gov/public/attachments/FCC-24-120A1.pdf.

Synopsis

I. DISCUSSION

In this *Report and Order*, we take a number of steps to support the STIR/SHAKEN framework and promote trust in our country's voice networks. We do so by authorizing providers with a STIR/SHAKEN implementation obligation to work with third parties to perform the technological act of signing calls to fulfill their compliance obligations under the Commission's rules, but establishing clear limits to ensure that such third-party arrangements neither undermine adherence to the requirements of the STIR/SHAKEN technical standards nor allow providers to avoid accountability for noncompliance. By "STIR/SHAKEN implementation obligation," we mean the applicable requirement under the Commission's rules that a provider implement STIR/SHAKEN in the IP portions of their networks by a date certain, subject to certain exceptions. When referencing those providers "without" a STIR/SHAKEN implementation obligation, we mean those providers that are subject to an implementation extension, such as a provider with an entirely non-IP network or one that is unable to obtain the necessary SPC token to authenticate caller ID information, or that

are exempted from our caller ID authentication requirements because they lack control over the network infrastructure necessary to implement STIR/SHAKEN. First, we define "third-party authentication" for the purposes of the rules we adopt today. Next, we limit the third-party authentication arrangements authorized under the Commission's rules to those in which the provider with the STIR/SHAKEN implementation obligation: (1) makes all attestation level decisions, consistent with the STIR/SHAKEN technical standards; and (2) ensures that all calls are signed using its own certificate obtained from a STIR/SHAKEN Certificate Authority—not the certificate of a third party. Utilizing a third party to sign traffic without complying with the requirements we adopt today will constitute a violation of the Commission's caller ID authentication rules. We further require that any provider certifying to partial or complete STIR/SHAKEN implementation in the Robocall Mitigation Database must be registered with the STIR/SHAKEN Policy Administrator, obtain its own SPC token from the Policy Administrator, use that token to generate a certificate with the Certificate Authority, and authenticate all its calls with that certificate, whether directly or through a third party. We also adopt recordkeeping requirements regarding third-party authentication arrangements to ensure compliance with the rules we adopt today and promote accountability in the event that any such arrangement leads to abuse of the voice network. Based on our review of the record, we find that taking these steps will enable providers to obtain the economic and other benefits of utilizing third-party technical solutions for STIR/SHAKEN implementation without compromising the integrity of the STIR/SHAKEN technical standards and governance model. This, in turn, will protect consumers by promoting more ubiquitous and accurate caller ID authentication.

A. Authorizing Third-Party Authentication Subject to Limitations to

Prevent Abuse

1. Defining the Scope of Third-Party Authentication

We first define "third-party authentication" for the purposes of the rules we adopt today, and also delineate the types of providers that are covered by the rules. In the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), we sought comment on the types of third-party arrangements being used by providers, including whether providers are entering into agreements with third parties to perform all or part of their authentication responsibilities. We sought specific comment on the solutions detailed in the 2021 Small Providers Report produced by the NANC, which described third-party solutions that providers could engage to perform the technological act of signing calls, including "hosted SHAKEN" services offered in a public or private cloud and "carrier SHAKEN" services in which calls are signed by an intermediate provider. As described in the NANC Report, in both of these scenarios, the provider with the STIR/SHAKEN implementation obligation determines the appropriate attestation level for a call and the third-party solution signs the call using the obligated provider's token. We also sought comment on several scenarios addressed in the ATIS-1000088 Technical Report in which a provider with a STIR/SHAKEN implementation obligation lacks a direct relationship with the end user of the voice service. These scenarios involve circumstances where the end user of the voice service is not the same as the "customer," as defined by the ATIS -1000088 Technical Report, such as when a wholesale provider originates a call onto the public network for its reseller customer that initiated the call on behalf of an end user. ATIS-1000088 defines "customer" as "[t]ypically a service provider's subscriber, which may or may not be the ultimate end-user of the telecommunications service." Under this definition, a customer "may be a person, enterprise, reseller, or value-added service provider." An "end-user" is defined as "[t]he entity ultimately consuming the VoIP-based telecommunications service," which may be

"the direct customer of [an originating] service provider or may indirectly use the VoIP-based telecommunications service through another entity such as a reseller or value-added service provider." ATIS-1000088, therefore, makes clear that, in some cases, the "customer" and "end user" are not the same. We additionally sought comment on whether we should limit any rule authorizing third-party authentication to the scenarios discussed by the Small Providers Report or those in the ATIS-1000088 Technical Report, or take a broader approach.

Based on our review of the record, and for the purposes of the rules we adopt today, we define "third-party authentication" to refer to scenarios in which a provider with a STIR/SHAKEN implementation obligation under the Commission's rules enters into an agreement with another party—a "third party"—to perform the technological act of signing calls on the provider's behalf. This definition of third-party authentication includes, for example, the "hosted SHAKEN" and "carrier SHAKEN" solutions that are described in the Small Providers Report. It excludes instances in which a provider with a STIR/SHAKEN implementation obligation authenticates its own traffic, and simply has a customer that is not the end user that initiated the call. We find that this definition is consistent with the caller ID authentication roles defined by the Commission's rules and the ATIS standards, and will establish a clear scope for the third-party authentication practices we authorize herein.

The Commission's rules establish three categories of providers with STIR/SHAKEN caller ID authentication obligations: (1) voice service providers that originate calls; (2) non-gateway intermediate providers that carry or process the calls without originating or terminating them; and (3) gateway providers that receive calls from foreign originating or intermediate providers at their US facilities and transmit them downstream. The Commission's rules further state that the STIR/SHAKEN implementation obligation applies to providers with control over the network

infrastructure necessary to implement STIR/SHAKEN. Providers that meet these criteria are obligated to implement STIR/SHAKEN and are thus the entities that would be the "first parties" in any third-party authentication arrangement authorized by our rules, i.e., they are the parties with the ultimate compliance obligation. That compliance obligation does not change simply because the provider has an upstream customer (e.g., a reseller or a value-added service provider) that is not the ultimate end user of the voice service and does not itself have a STIR/SHAKEN implementation obligation, e.g., a reseller that qualifies for the STIR/SHAKEN exemption or a value-added service provider (VASP) that provides communications services that are ancillary to the voice service. A VASP may provide services such as arranging for telephone number assignments from a service provider to a particular customer of the VASP or for the VASP's use irrespective of customer. As is often true with respect to resellers, an "originating [service provider] typically knows the VASP customer and does not have direct knowledge" of the VASP's end users. In these scenarios, the Technical Report provides guidance on the steps a provider with STIR/SHAKEN implementation obligation must take to verify its customer's identity and right to use a number, as required to provide an A- or B-level attestation. For instance, in the context of voice service providers, we agree with CCA that "[w]here, consistent with ATIS standards, an originating service provider provides an attestation for calls from its own reseller or [VASP] customer, it is not engaging in third party authentication[; i]t is instead using its certificate to provide an appropriate attestation to traffic from its own customers." Stated differently, the originating service provider in that example is performing its own STIR/SHAKEN implementation obligation and is not acting as a third party for its upstream customer. Thus, if a wholesale provider originates a call onto the public network on behalf of a reseller customer that lacks control over the network infrastructure necessary to implement STIR/SHAKEN, it is the wholesale provider that has the STIR/SHAKEN implementation

obligation, not the reseller. In this scenario, the wholesale provider is obligated to use STIR/SHAKEN to authenticate the caller ID pursuant to its own obligation under the Commission's rules, not as a third party for the reseller that is exempt from STIR/SHAKEN implementation requirements. Our framework authorizes all providers with a STIR/SHAKEN implementation obligation, regardless of their position in the call path, and subject to the limitations we set in place, to engage a third party for the technological act of signing calls. Therefore, where an intermediate provider (either a non-gateway intermediate provider or gateway provider) has a STIR/SHAKEN implementation obligation, it may fulfill that obligation through a third party subject to these same rules.

We find that any other interpretation would be inconsistent with the requirements for making attestation-level decisions when authenticating calls in the ATIS standards and reference documents. ATIS-1000074 only permits A- and B-level attestations to be made by providers that originate calls onto the IP-based service provider network. Although not defined in ATIS-1000074, that standard uses the term originating service provider, or OSP, consistent with related standards documents, such as ATIS-1000089, which defines originating service provider as: "[t]he service provider that handles the outgoing calls from a customer *at the point at which they are entering the public network*. The OSP performs the SHAKEN Authentication function." Thus, when an originating service provider authenticates a call based on what it knows about its customer and its customer's right to use a telephone number, it is performing its own STIR/SHAKEN implementation obligation, not that of its upstream customer in a third-party capacity. In these circumstances, it is the responsibility of the originating service provider to utilize reasonable "Know Your Customer" (KYC) protocols to establish a credible evidentiary basis for a "direct authenticated relationship with [its] customer" and/or verification of its customer's right to use the telephone number appearing in the caller ID field, sufficient to

apply an A- or B-level attestation under the ATIS standards. USTelecom, CTIA, and Numeracle urge us to adopt a definition of the term "customer" that is narrower than the one employed by the ATIS standards and reference documents. Specifically, they ask that we define "customer" to mean solely the end user that initiated the voice service, whether an individual or organizational entity. We decline to do so at this time because it is not necessary for the purposes of the third-party authentication rules we adopt today. We make clear above that the "first party" within any third-party arrangement is the entity with a STIR/SHAKEN implementation obligation, which under our existing rules and precedent, will necessarily be a voice service provider, intermediate provider, or gateway provider with control over the network infrastructure necessary to implement STIR/SHAKEN. As explained herein, whether the provider's customer is the ultimate end user of the voice service or another upstream entity is not dispositive of whether the provider has a STIR/SHAKEN implementation obligation and whether it may enter into an agreement with a third-party to perform the technological act of signing calls in fulfillment of that obligation subject to the requirements we adopt today. Further, we agree with NCTA, CCA, INCOMPAS, and ACA Connects that narrowing the definition of "customer" to mean solely the entity that initiates the voice service would be a significant departure from a plain reading of the ATIS standards and reference documents, and could be disruptive to the use cases that those standards and reference documents clearly contemplate as functioning within the STIR/SHAKEN ecosystem. ZipDX asks us to provide clarification as to the operation of our rules, including applicable KYC requirements, in a variety of hypothetical caller ID authentication arrangements. We decline to do so at this time, and find that commenting further on any given permutation of an authentication arrangement absent a more focused record on these matters would be unproductive. As we have explained above, the guidance we provide in this Order aligns with the text of the ATIS standards, including those which

contemplate more complex calling arrangements between resellers and wholesalers such as those ZipDX describes.

We thus decline ZipDX's suggestion that we incorporate providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN as first parties under this framework when they "hold [themselves] out as the originating service provider (even though [they] do[] not actually 'touch' the call)" and "arrange for somebody (the infamous third party) to sign the calls" for them. For the reasons discussed above, such a fluid conception of "originating service provider" would conflict with the text of the Commission's rules establishing the scope of providers subject to a STIR/SHAKEN implementation obligation and would be inconsistent with how the ATIS standards and technical reports use that term. We similarly reject other commenters' understanding of "third-party authentication" that describe scenarios in which a provider without a STIR/SHAKEN implementation obligation, such as a provider that lacks control over the network infrastructure necessary to implement STIR/SHAKEN, would be considered the "first party." We understand that there are currently voice service resellers that are voluntarily attempting to authenticate caller ID information despite not having control over the network infrastructure necessary to implement STIR/SHAKEN and, thus, lacking a STIR/SHAKEN implementation obligation under the Commission's rules. We understand that they often do so by relying on their wholesale providers to sign their calls. As explained above, such arrangements do not fall within the definition of third-party authentication that we adopt today, except insofar as the wholesale provider with the STIR/SHAKEN implementation obligation opts to use a third party to perform the technological act of signing calls on its behalf. We nevertheless encourage voice service resellers engaged in any form of authentication arrangement with wholesalers to provide such wholesalers with enough information to enable them to determine the appropriate attestation level of the calls initiated by the resellers' end users, pursuant to

the wholesaler's obligations under the Commission's rules and the STIR/SHAKEN standards.

2. Authorized Third-Party Authentication Practices

We next authorize providers with a STIR/SHAKEN implementation obligation to enlist the help of a third-party subject to certain conditions. In the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), we sought comment on whether we should amend the Commission's rules to explicitly authorize third-party authentication and what, if any, limitations we should place on that authorization to ensure compliance with authentication requirements and the reliability of the STIR/SHAKEN framework. Based on the evidence in the record, we permit providers with a STIR/SHAKEN implementation obligation under the Commission's rules to engage third parties to perform the technological act of signing calls as required by the STIR/SHAKEN standards, subject to two conditions: (1) the provider with the implementation obligation must make all attestation-level decisions, consistent with the requirements of the technical standards; and (2) all calls must be signed using the certificate of the provider with the implementation obligation. Relying on third parties to sign traffic without complying with these requirements will constitute a violation of the Commission's caller ID authentication rules. The rules we adopt today are not limited to arrangements based on a "Hosted SHAKEN" model or the "Carrier SHAKEN" model, or any other particular technological solution. We agree with TransNexus that limiting third-party authentication to currently existing technical solutions is unnecessary and may even inadvertently prevent innovation should new solutions be developed in the future. We will monitor any new solutions that may develop and may revisit this subject should action to address new risks be warranted. As explained below, we find that this approach will ensure the accountability necessary to maintain trust in the STIR/SHAKEN framework and will promote accurate and reliable A- and B-level attestations.

Commenters broadly agree that there are benefits to third-party authentication. Numeracle notes that third-party authentication is "necessary and beneficial for the timely and efficient implementation of STIR/SHAKEN." INCOMPAS adds that, "[e]ngaging in third-party caller ID authentication benefits the STIR/SHAKEN ecosystem by increasing the number of calls that are signed with a SHAKEN signature and by expanding the variety of signing options available to voice service providers and their customers." According to USTelecom, "for some providers, including smaller providers with limited resources, relying on third parties is essential to deploy STIR/SHAKEN in a cost-effective way. In addition, for certain equipment, including legacy IP equipment, third-party signing can be an effective and efficient means to deploy signing capabilities that otherwise would be cost-prohibitive." USTelecom's assertion accords with the NANC Small Providers Report, which concludes that third-party authentication may benefit small providers by reducing the costs associated with STIR/SHAKEN implementation.

The record also indicates, however, that certain types of third-party authentication practices can undermine confidence in the STIR/SHAKEN framework, and that guardrails are necessary. TransNexus argues that arrangements in which a "downstream transit provider authenticates calls using its own STI certificate and its specific means to determine the attestation level" present serious problems by "undermin[ing] STIR/SHAKEN and robocall prevention," and "enabl[ing] bad actors . . . to hide illegal robocalls amidst other calls authenticated by the transit provider." ACA Connects adds that "[t]hird-party call authentication could raise serious concerns in some contexts, including in situations where a provider employs a third-party for call authentication as a ploy to avoid scrutiny and accountability." NTCA similarly argues that, "[w]hile [third-party services] are a valuable option for providers' compliance with the Commission's caller-ID authentication rules, the potential for bad actors to utilize certain variations of

these arrangements in a way that could undermine the integrity of the STIR/SHAKEN ecosystem cannot be overlooked." NTCA and USTelecom agree that safeguards "are necessary to maintain trust in the STIR/SHAKEN ecosystem and allow these arrangements to function as intended for legitimate providers."

We thus balance the benefits and concerns associated with third-party authentication by adopting a rule that allows the practice subject to the two conditions specified above: (1) the provider with the STIR/SHAKEN implementation obligation must make all attestation-level decisions, consistent with the requirements of the technical standards; and (2) all calls must be signed using the certificate of the provider with the implementation obligation. We disagree with TransNexus's argument that we should simply issue a declaratory ruling to clarify that the Commission's rules already require voice service providers and intermediate providers to ensure that calls that they initiate onto the voice network are signed with their certificate, and to make all attestation-level decisions, regardless of which entity actually performs the act of signing. We instead find that codifying the rules through this *Eighth Report and Order* will not only ensure that all parties are the same page regarding their STIR/SHAKEN implementation obligations moving forward, but will also give us additional enforcement tools in the event a bad actor originating service provider attempts to hide behind a third party to obscure its identity. These key guardrails will allow providers to realize the benefits of third-party authentication without compromising the integrity of the trust and governance structure upon which STIR/SHAKEN relies. They will ensure that responsibility for properly authenticating a call's caller ID information—including complying with the attestation requirements of the ATIS standards—remains with the party assigned the STIR/SHAKEN implementation obligation under the Commission's rules, and will prevent providers from shirking their due-diligence duties by shifting STIR/SHAKEN authentication procedures to third parties. Under this approach,

originating service providers that rely on delegate certificates to establish a customer's right to use a telephone number, as required for an A-level attestation, may continue to do so to the extent permitted by the ATIS standards. These delegate certificates "provid[e] an end user or other VoIP entity with the ability to create and sign a PASSporT on its calls using a set of credentials . . . associated with [the] delegate certificate that is specific to the telephone number resources [which] that end user or other VoIP entity is authorized to use," though originating service providers may choose to "ignor[e] all PASSporTs signed with delegate certificate credentials." Because the originating service provider is ultimately responsible for making all attestation-level decisions and providing that information to a third-party performing the technological act of signing a call, the originating service provider remains responsible for vetting their customers and the criteria for applying A-level attestations, whether or not a delegate certificate is accepted. We decline SOMOS' suggestion that we should mandate acceptance of delegate certificates by providers in this *Eighth Report and Order*, as such a mandate is beyond the scope of the third-party authentication rules that we adopt today and the record in this proceeding is insufficient to weigh the benefits and burdens of imposing such a requirement. By requiring calls to be signed using the certificate of the provider with the implementation obligation, the STIR/SHAKEN governance model will be able to function as intended by making it easier to identify providers responsible for any authentication information transmitted with a call and facilitating enforcement remedies that may be needed for failures to comply with authentication requirements, including, for example, revocation of a provider's SPC token by the Secure Telephone Identity Governance Authority (STI-GA). We agree with commenters that the sharing of a provider's certificate with a third-party authenticator for the purpose of populating the identity header of a call does not create a security risk or undermine the STIR/SHAKEN trust model. As TransNexus states, STIR/SHAKEN certificates are similar to other

secure certificates used extensively on the Internet: "Most certificate holders provision their certificates and private keys to be hosted by third parties. These companies are experts in securing digital assets, and they use technology best practices and systems to minimize risks." Further, we conclude that a provider's direction to a third-party authenticator as to which attestation level to apply to a given call does not raise concerns about privacy or confidentiality. As Numeracle confirms, "the service provider should be able to pass its direction for attestation on to systems maintained by vendors used for technical support to apply the appropriate attestation level to the service provider's own calls without having to also supply its [third-party authenticator] with contextual data related to its decision." NCTA states that any information that may need to be shared "is typically no more information than would be shared in connection with other robocall mitigation efforts, such as traceback or other initiatives to combat abusive calling practices . . . ." No commenter argues third-party authentication practices, or specifically the sharing of information and certificates with third parties to perform the technological act of signing calls, presents security, privacy, or confidentiality concerns. A few commenters note that the STI-GA is working on ways to address "improper attestations," and last year published a document providing guidance regarding what it considers to be "improper attestation," to "support STI GA processes and policies," including its token revocation process. By adopting guardrails on third-party authentication practices and ensuring that all calls are signed with the token of the provider with the STIR/SHAKEN implementation obligation, rather than a third party that may perform the technological functions of signing a call for that provider, we assist in the STI-GA's effort to address improper attestation by increasing transparency.

We find that this approach will also guard against improper A- and B-level attestations by parties that are not originating service providers. Under the ATIS standards, an A- or B-level attestation can only be applied if the provider authenticating

the call originates it onto the public network. That ATIS criterion can be satisfied in the context of a third-party arrangement where the originating service provider either: (1) arranges with a third party to perform the technological act of signing a call before the provider originates the call onto the public network; or (2) originates the call onto the public network with an agreement in place for a downstream intermediate provider to perform the technological act of signing the call. The second requirement of A- and B-level attestation, i.e., confirmation that an originating service provider has a "direct authenticated relationship" with its customer and can identify the customer, is a determination that cannot be made by a third party with no relationship to that customer. The last requirement for an A-level attestation, i.e., confirmation that the originating service provider has established that the customer has a legitimate right to use the telephone number that appears in the caller ID, also necessarily requires due diligence by the originating service provider. We thus agree with commenters in the record that it is inconsistent with the Commission's rules and the ATIS standards to allow third parties to make such determinations. Since, as discussed above, the calls will need to be signed using the originating service provider's certificate, the rules we adopt today will ensure that such originating service providers are held accountable for improper attestation-level decisions for the calls they originate onto the public network, even if the technological act of signing the calls is performed by a third party.

Commenters generally support our adoption of these guardrails. CTIA and Numeracle argue that this approach "is consistent with the existing [ATIS] standards and the FCC's regulatory framework for STIR/SHAKEN implementation." CTIA also notes that requiring the use of "an originating [service] provider's [certificate] will better achieve the goals of the STIR/SHAKEN framework to promote a trusted voice ecosystem and increase transparency and integrity of caller ID information." USTelecom contends that, "when calls are signed with the originating [service] provider's token, the

Commission, the provider community, and analytics providers will have the information they need to take action should an originating [service] provider prove to routinely originate and authenticate illegal robocalls . . . ." TransNexus argues that such limitations will, *inter alia*, "improve the quality of caller [ID] authentication information available to terminating providers," and thereby improve their call analytics.

We are not persuaded, however, by the arguments advanced by the few commenters that oppose the guardrails we adopt today. INCOMPAS argues that we should not adopt any rules governing third-party authentication, and specifically opposes requiring providers to ensure that third-party authenticators sign calls using the provider's certificate. INCOMPAS implies that third-party authentication arrangements using the third party's certificate, rather than the originating service provider's, do not impede traceback efforts because "domestic originating providers . . . typically are identified to the Industry Traceback Group ('ITG') by the signing company" in such arrangements, and use of an origination identifier or "origID" by third-party signing providers would be sufficient to "ensure that the Commission or ITG can identify the source of any illegal robocalls." We disagree. The origID field is an "opaque identifier" that "does not convey any [service provider] or customer information in and of itself." Moreover, use of the origID field is permitted, but not required, by the ATIS standards, which do not establish detailed specifications regarding its use by providers. The approach described by INCOMPAS requires the ITG to obtain the cooperation of a third-party signing provider before it can identify the originator of an illegal call. In contrast, requiring third-party signers to use the originating service provider's token will allow the ITG to directly identify the originating service provider, thereby improving the efficiency of the traceback process and accountability within the STIR/SHAKEN ecosystem. INCOMPAS argues that instead we should "rely on the authority of the Enforcement Bureau to address those instances when an illegal robocaller is attempting to evade

accountability through third-party authentication[, and] . . . rely on the [STI-GA] to address any ongoing issues or gaps in the standards that lead to attestation abuse." We are committed to enforcing the Commission's rules against illegal robocallers and agree that the STI-GA should exercise its authority to hold providers accountable for non-compliance with the ATIS standards. That does not mean, however, that we should not proactively adopt common-sense guardrails to prevent abuse of third-party authentication arrangements. By codifying these new rules, we give more certainty to providers seeking to comply with our caller ID authentication framework, establish clear standards that the Enforcement Bureau can apply when investigating misconduct, and enable the STIR/SHAKEN ecosystem to realize additional benefits, such as making authentication information more valuable for call analytics. We thus reject INCOMPAS's inference that it is sufficient to simply rely on providers to voluntarily establish appropriate parameters for the application of STIR/SHAKEN technical standards in commercial arrangements with third parties. As discussed below, we require all third-party authentication arrangements to be memorialized in written agreements that comport with the rules we adopt today. INCOMPAS and VON also argue that changes to the Commission's rules may risk creating regulatory conflict with foreign jurisdictions, but provide no detail as to why imposing guardrails on third-party authentication would cause such an issue. While we acknowledge that maintaining "interoperability among SHAKEN systems internationally" is certainly important in protecting domestic consumers from illegal robocalls originating abroad, our action today eliminates the risk of such regulatory conflict by remaining consistent with the ATIS standards.

B. Implementation and Compliance Requirements

In this Section, we adopt several implementation requirements for providers that utilize third-party authentication and amend certain rules to comport with those requirements. In the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May

5, 2023), the Commission sought comment on whether any other rules would need to be amended if it explicitly authorized third-party authentication. Specifically, and as described below, we require all providers with a STIR/SHAKEN implementation obligation to: (1) obtain an SPC Token and digital certificate; (2) certify to complete or partial implementation in the Robocall Mitigation Database *only* if they have obtained an SPC token and digital certificate and sign calls with their certificate; and (3) memorialize and maintain records of any third-party authentication agreement(s) they have entered into, subject to certain limitations.

Requirement to Obtain a Token and Digital Certificate. Consistent with the third-party authentication rule we adopt today, all providers with a STIR/SHAKEN implementation obligation under the Commission's rules will now be explicitly required to obtain an SPC token from the Policy Administrator and present that token to a STIR/SHAKEN Certificate Authority to obtain a digital certificate. This requirement is necessary now that all calls, whether technologically signed directly by the provider with the STIR/SHAKEN implementation obligation or by a third party, must be signed with the former's certificate, thereby ensuring that accountability for compliance with our caller ID authentication rules remains with the party required to implement STIR/SHAKEN under the Commission's rules. The record indicates that requiring all providers with a STIR/SHAKEN implementation obligation to obtain their own SPC tokens and digital certificates will also result in other benefits, such as "encourag[ing] continued innovation" within the existing STIR/SHAKEN framework and ensuring that providers with STIR/SHAKEN implementation obligations under the Commission's rules "have a fair and proportionate financial stake in the STIR/SHAKEN ecosystem." We believe the positive effects of this requirement will be far-reaching, as the record indicates that many providers claiming to have implemented STIR/SHAKEN have not obtained their own tokens and certificates. Indeed, TransNexus estimates "that about

64% of providers" in the Robocall Mitigation Database that claim STIR/SHAKEN implementation are not registered with the Policy Administrator.

We disagree with INCOMPAS that "requiring all providers to obtain a token that could be used by a third-party authenticator would necessitate changes with both the industry's token access policies and the Commission's current administration of voice service providers." In support of its arguments, INCOMPAS merely lists the STI-GA's SPC token access standards, including the requirement to obtain an Operating Company Number (OCN), and states that many providers "do not operate a business model that allows them to get an OCN." INCOMPAS does not, however, explain why this would be the case for any provider with a STIR/SHAKEN implementation obligation, much less "many" providers with STIR/SHAKEN implementation obligations. In fact, in recent years, the Wireline Competition Bureau has repeatedly found that few providers are currently unable to obtain an SPC token due to revisions made to the STI-GA token access policy in May 2021. Consistent with this finding, the record in this proceeding evidences that the barriers to and costs associated with obtaining and maintaining SPC tokens and digital certificates are low, including for small providers. Moreover, the compliance deadline we adopt below provides ample time for all sizes of providers to come into compliance with our newly adopted rules, thereby minimizing any compliance burdens. While INCOMPAS states that some providers are unable to get an OCN "from the Commission," OCNs are assigned by the National Exchange Carrier Association (NECA). INCOMPAS also states that "voice service providers are required to provide the STI Policy Administrator with all-associated IP addresses as part of acquiring a Service Provider Code token," and claims that this is a highly burdensome step. INCOMPAS does not explain why supplying IP addresses to the Policy Administrator is highly burdensome, however, or why any burden of submitting the information would outweigh the benefits of requiring providers with a STIR/SHAKEN implementation

obligation to register with the Policy Administrator. We note that the Policy Administrator states that it collects IP addresses from providers for the purpose of whitelisting. According to the National Institute of Standards and Technology's Computer Security Resource Center (CSRC), a whitelist can be defined as "[a]n approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition." We note that providers that cannot obtain an SPC token after diligently pursuing one from the Policy Administrator may still claim an implementation extension under the Commission's existing rules. While the Commission sought comment on whether to eliminate the SPC token extension in the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), we decline to do so at this time. In March 2023, the Commission updated its requirements for submissions to the Robocall Mitigation Database, including a new requirement that providers claiming a STIR/SHAKEN implementation extension or exemption explicitly state the rule that excepts it from compliance and why the provider qualifies for the extension or exemption. All providers were required to file submissions to the Robocall Mitigation Database that comply with this and additional content requirements by February 26, 2024. These filings are currently under review. As part of that assessment, the Wireline Competition Bureau will determine the number of providers still relying on the SPC token extension and the merit of the justifications submitted by those claiming the extension. We will be better able to determine whether to retain or eliminate the SPC token extension at that time.

Robocall Mitigation Database Certifications. Consistent with the foregoing requirements, we update the Commission's rules to prohibit any provider with a STIR/SHAKEN implementation obligation from certifying to complete or partial implementation in the Robocall Mitigation Database unless they have obtained an SPC token and digital certificate and sign calls with their certificate, either themselves or when

working with a third party to perform the technological act of signing calls having met the necessary conditions we impose in this Order. In the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), the Commission sought comment on whether it should "prohibit providers from certifying to having implemented STIR/SHAKEN in the Robocall Mitigation Database unless their calls are signed with their own SPC token, whether directly or through a third party." For all of the reasons discussed above, we agree with TransNexus that providers that have a STIR/SHAKEN implementation obligation but rely on third-party authentication arrangements using the third party's certificate are not in compliance with the governance model established by STIR/SHAKEN technical standards, which require providers to obtain an SPC token and digital certificate to authenticate calls. Such providers should not, therefore, claim to have implemented STIR/SHAKEN pursuant to the technical standards required by the Commission's rules in the Robocall Mitigation Database. While we recognize that some of these providers may have relied on third-party SPC tokens and certificates out of a good faith belief that such arrangements are permissible under the Commission's rules in the past, such practices will now be expressly prohibited by our rules, and providers that have relied on third-party tokens and digital certificates in the past will now need to obtain their own SPC tokens and certificates and use them to sign calls, consistent with the requirements of the STIR/SHAKEN standards and the compliance deadlines we set below. Providers that do not obtain and use an SPC token and certificate must update their Robocall Mitigation Database certifications to state that they have not fully or partially implemented STIR/SHAKEN to avoid being referred to the Enforcement Bureau for violations of the Commission's rules, including the rules governing certifications submitted to the Robocall Mitigation Database and the obligation to submit information to the Commission that is true, accurate, and up-to-date. Providers that qualify for a STIR/SHAKEN implementation extension because they cannot satisfy the requirements

to obtain an SPC token can claim the extension in their Robocall Mitigation Database submissions at this time.

We decline to adopt new content requirements for Robocall Mitigation Database certifications at this time. In the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), the Commission sought comment on requiring providers to submit additional information to the Robocall Mitigation Database, "including the identity of the third party providing [their authentication] solution, any requirements the provider has imposed on the third party to ensure compliance with the requirements of the ATIS technical standards and the Commission's rules, and what the provider itself does to ensure compliance with those requirements under the third-party arrangement[.]" In response to the *Further Notice*, commenters suggest that we should require providers to submit a variety of additional information to the Robocall Mitigation Database, including evidence of registration with the Policy Administrator, the identity of any third-party authentication solutions they use, and information that details their Know Your Customer standards.

We conclude that any value of requiring providers to submit this information at this time is minimal, and does not warrant the additional operational and administrative burdens of requiring providers to update their Robocall Mitigation Database submissions. For instance, now that we require all providers with a STIR/SHAKEN implementation obligation to obtain their own SPC token from the Policy Administrator and a digital certificate from a Certification Authority, we conclude it unnecessary for providers to make a further showing at this time that they are registered with the Policy Administrator, as TransNexus suggests. Moreover, as Numeracle points out, the Policy Administrator's list of providers authorized to participate in STIR/SHAKEN is publicly available, allowing Commission staff to easily verify a provider's registration status without further expanding the Robocall Mitigation filing requirements. We also believe it is unnecessary

to require providers to identify any third-party authentication solutions they use in their Robocall Mitigation Database submissions, as NCTA suggests. Under the rules we adopt today, which require calls to be signed using the digital certificate of the provider with the STIR/SHAKEN implementation obligation, responsibility and accountability for compliance with the STIR/SHAKEN standards will be traced back to that provider, not a third-party entity that technologically signs the call. Further, we agree with INCOMPAS that requiring providers to identify the specific third-party solutions that they may employ to perform the technological act of signing calls could require providers to update their Robocall Mitigation Database submissions more frequently if such solutions change, thereby increasing administrative burdens for providers with minimal benefit. Lastly, providers are already required to describe in their robocall mitigation plans how they comply with their existing obligation to know their customers under the Commission's rules. We, thus, decline to further amend our requirements for Robocall Mitigation Database certifications at this time, but we will closely observe how providers comply with the requirements we adopt today to determine whether additional information would assist our compliance reviews and enforcement activities in the future. ZipDX proposes that "[n]ew [Robocall Mitigation Database] registrations should not immediately become active. Instead, FCC staff should vet the registration to ensure that the applicant has a token from the STI-PA and if not, that the filed RMP contain a thorough, credible explanation as to why not." In August 2024, we launched a separate proceeding to consider procedural measures for improving the overall quality of information submitted to the Robocall Mitigation Database. We believe that addressing ZipDX's procedural proposal would be more appropriate in the context of that proceeding, and thus decline to do so here. ACA Connects argues that the "Commission could further require reseller providers to disclose to the Commission (on a confidential basis), the identity of any wholesale provider that authenticates some or all of their calls." As discussed above,

however, in the context of a wholesale provider originating a call onto the public network for a reseller which lacks control over the network infrastructure necessary to implement STIR/SHAKEN, it is the wholesale provider that has the STIR/SHAKEN implementation obligation, that must authenticate the calls using its own digital certificate.

Recordkeeping. To ensure compliance with the requirements we adopt herein for third-party authentication, and to enable the Commission to monitor such compliance and enforce its rules, we require that providers that choose to work with a third party to perform technological act of signing calls do so pursuant to a written agreement. In the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), the Commission sought comment on the measures it would "need to implement to monitor compliance with its rules if third-party authentication arrangements are employed." No commenter raises arguments for or against recordkeeping requirements. The required written agreement must specify the specific tasks that the third party will perform on the provider's behalf and confirm that provider will: (1) make all attestation-level decisions for calls signed pursuant to the agreement, and (2) ensure that all calls will be signed using the provider's certificate. Providers may be required to submit a copy of the agreement to the Commission in connection with a review of the provider's compliance with the Commission's rules or an investigation by the Enforcement Bureau. To the extent that an agreement between a provider with the STIR/SHAKEN implementation obligation and a third party contains confidential information, providers may seek confidential treatment for that information. We require that a current agreement be in place for as long as any third-party authentication arrangement exists, and that all copies of third-party agreements be maintained for a period of two years from the end or termination of the agreement. We emphasize that there must be a memorialized agreement between the provider with the STIR/SHAKEN implementation obligation and the third party performing the technological act of signing a call for the arrangement to be

considered third-party authentication under the rules we adopt today. For example, the Commission's rules require voice service providers to authenticate the traffic that they originate, and, if they fail to do so, non-gateway intermediate providers must themselves authenticate any unauthenticated calls they receive directly from originating providers. Consequently, an intermediate provider that receives an unauthenticated call from an originating provider does not engage in third-party authentication simply because it is the entity that uses STIR/SHAKEN to authenticate the call. In such an instance, the intermediate provider is discharging its own authentication obligation under the Commission's rules by signing the unsigned traffic. For this reason, we do not share ZipDX's concern about a lack of accountability for calls in the event that a wholesale provider might claim that it should be "deemed an intermediate provider" in relation to a reseller customer. If, however, the originating service provider has executed an agreement for its immediate downstream intermediate provider to perform the technological act of signing a call on the originating provider's behalf, subject to the conditions adopted in this *Eighth Report and Order*, that would qualify as a third-party authentication arrangement. We thus reject INCOMPAS's argument that our definition of third-party authentication should apply when downstream providers are merely "signing calls that were not signed up-stream," even if the downstream provider "may not be offering signing service *per se*."

Compliance Deadline. The new third-party authentication guardrails we adopt in this *Report and Order* include recordkeeping and Robocall Mitigation Database certification requirements under 47 CFR 64.6301(b)(3)-(b)(5), 64.6302(f)(3)-(f)(5), and 64.6305(d)-(f), which may contain new or modified information collections subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA). While the remaining amendments to §§ 64.6301 through 64.6305 adopted in this *Report and Order* do not themselves require OMB approval, in practice, compliance

with the requirements of these provisions will likely entail compliance with the provisions of 64.6301(b)(3) through (5), 64.6302(f)(3) through (5), and 64.6305(d) through (f), respectively. Therefore, we set a compliance deadline for all our newly adopted requirements of 30 days after publication of this *Report and Order* in the *Federal Register* following OMB approval, or 210 days after release of this *Report and Order*, whichever is later.

We expect that requiring providers to comply with all of the obligations we adopt in the *Report and Order* on the same date will facilitate compliance with our rules, and consequently we elect to delay the effectiveness of the entirety of the modifications to §§ 64.6301 through 64.6305 pending OMB approval of §§ 64.6301(b)(3) through (5), 64.6302(f)(3) through (5), and 64.6305(d) through (f). Consistent with the Commission's approach in prior rulemakings, we direct the Wireline Competition Bureau to announce effective dates for 47 CFR 64.6301 through 64.6305 through Public Notice. Any provider with a STIR/SHAKEN implementation obligation that has failed to both: (1) obtain an SPC token from the Policy Administrator and a digital certificate from a Certificate Authority; and (2) ensure that all calls that it is required to authenticate are signed using its own digital certificate, will be required to update their certifications in the Robocall Mitigation Database to state that they have not fully or partially implemented STIR/SHAKEN by the effective date of the rules listed in this paragraph as announced by Public Notice.

The record reflects support for our adoption of a single compliance deadline for our third-party authentication obligations based on the schedule above. Commenters explain that providers using third-party authentication solutions may have to make a number of commercial and network changes to comply with the newly adopted authentication and robocall mitigation requirements, such as creating new commercial arrangements with customers or third-party vendors, taking the steps needed to obtain a

token and certificate, determining the process for assigning an attestation level, and making changes to their network to sign calls with their own token. We agree with NCTA that adopting a transition period would "promote fairness and avoid exposing providers relying on good faith on non-conforming third-party solutions to the threat of immediate liability." We also agree with INCOMPAS that "[w]hile the evolution toward broad token access should be encouraged, expecting a flash-cut" to such a change would not be practical. Therefore, we grant providers a reasonable amount of time to adjust their third-party call authentication practices to comply with the rules we adopt today, and will not require compliance with these rules sooner than 210 days after release of this *Report and Order*. Although we find that this approach will allow sufficient time for providers to adjust their third-party authentication practices, providers should comply with our new rules as soon as reasonably practicable. In this instance, we agree with INCOMPAS and CCA that a period of at least 210 days following the release of this *Report and Order* will ensure that providers have sufficient time to achieve compliance with our new rules.

C. Summary of Cost-Benefit Analysis

We find that the benefits of the third-party authentication rules we adopt today will greatly exceed the costs they will impose on providers. In the *Sixth Caller ID Authentication Report and Order* (88 FR 29035, May 5, 2023), the Commission confirmed the conclusion that "our STIR/SHAKEN rules are likely to result in, at a minimum, $13.5 billion in annual benefits," and that the benefits associated with the rules will greatly outweigh the costs imposed on providers. We again affirm this conclusion, and find that "[l]imiting the ability of illegal robocallers to evade existing rules will preserve and extend the benefits of STIR/SHAKEN."

Benefit: Preserving the Structural Integrity of the STIR/SHAKEN Regime. Establishing clear rules of the road for providers using third parties to authenticate voice

service calls will increase the STIR/SHAKEN framework's benefits. Our new third-party authentication requirements will increase compliance with the Commission's caller ID authentication rules, promote accountability and trust within the STIR/SHAKEN framework, and improve the accuracy of A- and B- level attestations. As a result, more illegal robocalls will be identified and stopped before they can reach American consumers, helping increase confidence in the U.S. telephone network. In adopting these requirements, we strike a balance that allows providers to realize the benefits of third-party authentication while preventing abuses that could undermine the STIR/SHAKEN standards. The new rules will increase the number of calls signed with a SHAKEN signature, give providers and their customers more signing options, and make it more cost-effective for all providers to implement STIR/SHAKEN. Indeed, the record reflects that third-party authentication may "confer[] substantial benefits," particularly for small providers, as deploying STIR/SHAKEN in the IP portion of their voice service network may otherwise be cost-prohibitive. The cost savings that make third-party authentication a worthwhile, cost-effective investment for small providers is an added benefit.

Benefit: Ensuring Reliable Access to Emergency and Healthcare Communications. In the *First Caller ID Authentication Report and Order* (85 FR 22029, Apr. 21, 2020), the Commission noted that "hospitals and 911 dispatch centers have reported that robocall surges have disabled or disrupted their communications network, and such disruptions have the potential to impede communications in life-or-death emergency situations. In one instance, Tufts Medical Center in Boston received more than 4,500 robocalls in a two-hour period. In another, the phone lines of several 911 dispatch centers in Tarrant County, Texas, were disabled because of an hourlong surge in robocalls." Although the Commission declined then to estimate the considerable public safety benefits of reduced robocalling, in the wake of subsequent Commission orders estimating the public safety benefits of reduced emergency response delays, we elect to

do so now. In the *Location-Based Routing Report and Order* (89 FR 18488, Mar. 13, 2024), we estimated that a one-minute reduction in average emergency response times would save 13,837 lives, a mortality risk reduction worth $173 billion annually. Based on that figure, any reduction in emergency response delays caused by robocalls could confer large benefits. For example, if unwanted and illegally spoofed robocalls caused only a one-second delay in average emergency response times, the potential mortality risk-reduction benefit would be worth $2.88 billion annually (i.e., 173/60=2.88). Assuming a linear relationship between prevalence of robocalling and possible emergency response delays, a one-tenth reduction in robocalling and the accompanying tenth-of-a-second reduction in emergency response time, which could be achieved by better third-party authentication, would be worth $288 million annually. A more modest one-twentieth reduction in robocalling and one-twentieth-of-a-second reduction emergency response times would be worth $144 million annually. To achieve $100 million in annual public safety benefits, our third-party authentication rules would only have to reduce unwanted and illegal robocalls such that average emergency response times were improved by a mere 0.035 seconds, or about one-thirtieth of a second. Given the prevalence of robocalls and their ability to disrupt communications and cause network congestion, it is highly likely that implementing third-party authentication rules to strengthen the STIR/SHAKEN ecosystem will reduce robocalls by at least this much, resulting in life-saving benefits.

Benefit: *Reducing Network Congestion and Consumer Complaints.* The Commission has noted previously that unwanted and illegal robocalls increase network congestion and the labor costs of handling numerous customer complaints. Third-party-authenticated traffic that does not currently meet STIR/SHAKEN technical standards and results in illegal or unwanted robocalls terminates on the networks of unwitting carriers, forcing them to bear the costs of unwanted call traffic in the form of increased customer

complaints and network congestion. Tightening third-party authentication requirements will generate savings for voice service providers, which may pass them on to consumers in the form of lower rates.

Costs. While some argue that limitations on third-party authentication may be costly without concomitant benefits, the record more broadly reflects that the costs of requiring providers that use third-party solutions to authenticate calls with their own token and applying their attestation level to their calls will be minimal for all providers, including small providers. As explained above, by adopting a minimum compliance period for our third-party authentication requirements of 210 days following release of this *Report and Order*, we take a balanced approach that maximizes the benefits to providers using third-party authentication solutions while minimizing its costs. And, though we acknowledge that our adopted third-party authentication requirements will have implementation and recordkeeping costs, we conclude that explicitly authorizing third-party authentication with our adopted limitations will produce significant benefits, including increased trust in the STIR/SHAKEN framework and the accuracy of A- and B-level attestations.

D. Legal Authority

Consistent with our proposals, we adopt the foregoing obligations pursuant to the legal authority that the Commission relied on in prior caller ID authentication and call blocking orders. We note that no commenter questioned our proposed legal authority.

Third-Party Authentication. We conclude that Section 251(e) of the Act and the Truth in Caller ID Act provide us with the authority to authorize providers to engage in third-party authentication practices subject to certain limits. Specifically, we find that our Section 251(e) numbering authority and the Truth in Caller ID Act each provide the Commission with independent authority to require providers that use third parties to authenticate calls to adhere to two limitations: (1) the provider with the STIR/SHAKEN

implementation obligation under the Commission's rules must be the entity that determines whether A-, B-, or C- level attestation should be applied to the call; and (2) all calls must be signed using the SPC token of the provider with the implementation obligation.

As the Commission explained in the *First Caller ID Authentication Report and Order* (85 FR 22029, Apr. 21, 2020), Section 251 provides the Commission with exclusive, independent jurisdiction over numbering issues in the United States and "enables us to act flexibly and expeditiously with regard to important numbering matters[,]" including "[w]hen bad actors unlawfully spoof the caller ID that appears on a subscriber's phone[.]" Further, the Truth in Caller ID Act provides us with authority to adopt rules that are "necessary to . . . protect voice service subscribers from scammers and bad actors." As the Commission has found in several caller ID authentication and call blocking orders, we again find that Section 251(e) and the Truth in Caller ID Act provide the Commission with the authority "to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers[.]" The record reflects that the limitations on third-party authentication we adopt today are necessary to ensure the integrity of and trust in the STIR/SHAKEN ecosystem and will help shield customers from the scourge of illegal robocalls. Adopting rules for third-party authentication practices will also help prevent the fraudulent exploitation of the NANP by ensuring that the parties responsible for implementing STIR/SHAKEN under the Commission's rules remain accountable for meeting the STIR/SHAKEN standards. We thus find that Section 251(e) of the Act and the Truth in Caller ID Act provide us with the authority to adopt the foregoing third-party authentication rules.

Implementation and Compliance Measures. We conclude that the TRACED Act provides additional, independent authority to require providers to obtain an SPC token and sign their calls with their own certificate in order to satisfy a STIR/SHAKEN

implementation obligation under the Commission's rules. Congress expressly required the Commission to require voice service providers to implement the STIR/SHAKEN caller ID authentication framework in the TRACED Act. Consistent with the Commission's prior call blocking and caller ID authentication orders, we find that Sections 201(b) and 201(a) of the Act, and the Commission's ancillary authority in Section 4(i) of the Act, provide us with additional sources of authority to adopt these robocall mitigation requirements. Requiring providers to acquire their own SPC token from and register with the Policy Administrator, obtain a digital certificate from a STIR/SHAKEN Certificate Authority, and sign calls with their digital certificate will better ensure that providers are meeting their responsibilities to properly authenticate calls and comply with the requirements of the ATIS standards. Our third-party authentication rules will therefore help maintain the integrity of the trust and governance structure upon which STIR/SHAKEN relies, as these rules will better ensure that providers are held accountable for properly implementing STIR/SHAKEN. Adopting these requirements will thus increase the efficacy and trust of the call authentication framework that the TRACED Act required.

We also find that Section 251(e) of the Act and the Truth in Caller ID Act also provide us with the authority to adopt the implementation and compliance measures for the third-party authentication rules that we adopt in this *Report and Order*. Specifically, we conclude that Section 251(e) of the Act and the Truth in Caller ID Act authorize us to: (1) prohibit any provider from certifying to full or partial implementation in the Robocall Mitigation Database unless they have obtained their own SPC token and sign calls with their own digital certificate; (2) require that any third-party authentication arrangement be memorialized in an agreement between the party with the STIR/SHAKEN implementation obligation under the Commission's rules and the third-party signer; and (3) require the memorialized agreement be in place for as long as any third-party

authentication arrangement exists, and that all copies of third-party agreements be maintained for a period of two years from the end or termination of the agreement. As explained above with respect to our third-party authentication rules, these measures will help providers realize the benefits of third-party authentication while providing greater mechanisms for accountability that will ensure that providers are complying with their STIR/SHAKEN implementation obligations. Consequently, we find that these requirements will also prevent the fraudulent abuse of North American Numbering Plan (NANP) resources as directed in Section 251(e) of the Act, as well as protect voice service subscribers as directed in the Truth in Caller ID Act by increasing trust in the STIR/SHAKEN standards.

II. FINAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act of 1980 (RFA), as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Call Authentication Trust Anchor Further Notice of Proposed Rulemaking* released in March 2023 (*Sixth Caller ID Authentication Further Notice*) (88 FR 29035, May 5, 2023). The Federal Communications Commission (Commission) sought written public comment on the proposals in the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023), including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

A. Need for, and Objectives of, the Order

The *Eighth Report and Order* takes important steps in the fight against illegal robocalls by explicitly authorizing providers to use third-party authentication solutions to comply with their existing STIR/SHAKEN implementation obligations and adopting associated implementation and compliance measures. The decisions we make here protect consumers from unwanted and illegal calls while balancing the legitimate interests of callers placing lawful calls. First, the *Eighth Report and Order* requires a

provider that uses a third-party solution for signing calls to satisfy its STIR/SHAKEN implementation obligation under the Commission's rules to make the attestation-level decisions itself, and ensure that its calls are signed with its own certificate, rather than that of a downstream provider or other third party. Second, it requires all providers with a STIR/SHAKEN implementation obligation to: (1) obtain an SPC Token and digital certificate; (2) certify to complete or partial implementation in the Robocall Mitigation Database only if they have obtained an SPC token and digital certificate and ensure their calls are signed with their own certificate; and (3) memorialize any third-party authentication arrangement in an agreement and maintain a record of such agreement(s) for two years from the end or termination of the agreement, alongside certain additional requirements. These guardrails for third-party authentication arrangements will help to ensure providers remain accountable for complying with their STIR/SHAKEN implementation requirements and are transparent regarding their caller ID authentication practices.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

Though there were no comments raised that specifically addressed the proposed rules and policies presented in the *Sixth Caller ID Authentication Further Notice* (88 FR 29035, May 5, 2023) IRFA, the Commission did receive comments addressing the burdens on small providers. There is general agreement that the barriers to and costs associated with obtaining and maintaining SPC tokens and digital certificates are low for small providers. A few commenters argued that a compliance period of at least 210 days following release of this *Report and Order* would give the industry time to comply with any rules limiting third-party authentication. The Commission found that the commenters provided sufficient evidence to support adoption of a minimum 210-day compliance period for purposes of these rules.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which Rules Will Apply

The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "mall governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act. A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

Small Businesses, Small Organizations, Small Governmental Jurisdictions. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small

businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.

Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide, for tax year 2022, there were approximately 530,109 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand." U.S. Census Bureau data from the 2022 Census of Governments indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,845 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts) with enrollment populations of less than 50,000. Accordingly, based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 entities fall into the category of "small governmental jurisdictions."

Wired Telecommunications Carriers. The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network

facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband Internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Local Exchange Carriers (LECs). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590

providers that reported they were fixed local exchange service providers. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Incumbent Local Exchange Carriers (Incumbent LECs). Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers. Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

Competitive Local Exchange Carriers (LECs). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service

Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers. Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Interexchange Carriers (IXCs). Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

Cable System Operators (Telecom Act Standard). The Communications Act of 1934, as amended, contains a size standard for a "small cable operator," which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000. For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count

established in a 2001 Public Notice. Based on industry data, only six cable system operators have more than 677, 000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

Other Toll Carriers. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services. Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Wireless Telecommunications Carriers (except Satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this

industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Satellite Telecommunications. This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $35 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year. Of this number, 242 firms had revenue of less than $25 million. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services. Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees. Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

Local Resellers. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services. Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Toll Resellers. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are

included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services. Of these providers, the Commission estimates that 495 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Prepaid Calling Card Providers. Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications Resellers is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services. Of these providers, the Commission estimates that 57 providers have 1,500 or fewer

employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

All Other Telecommunications. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

The *Eighth Report and Order* requires providers that choose to engage in third-party authentication to do so subject to certain limitations. These changes affect small and large companies and apply to all the classes of regulated entities identified above. Specifically, the *Eighth Report and Order* authorizes providers to engage third parties to perform the technological act of signing calls, as required by the STIR/SHAKEN standards, provided that providers with a STIR/SHAKEN implementation obligation make all attestation-level decisions for calls authenticated by third-parties, and ensure that all calls authenticated using third-party solutions are signed using the certificate of

the provider with the STIR/SHAKEN implementation obligation under the Commission's rules.

The *Eighth Report and Order* also adopts implementation and compliance requirements, consistent with the above requirements for third-party authentication. First, providers with a STIR/SHAKEN implementation obligation must acquire their own SPC token and digital certificate. Second, these providers may only certify to complete or partial implementation in the Robocall Mitigation Database if they have obtained an SPC token and digital certificate and sign calls with their certificate, whether by themselves or through a third party.

Finally, the *Eighth Report and Order* also adopts a recordkeeping requirement for providers with a STIR/SHAKEN implementation obligation that enter into an arrangement with a third party to authenticate the provider's calls. It requires that any third-party authentication arrangement be memorialized in an agreement between the party with the STIR/SHAKEN implementation obligation under the Commission's rules and the third-party signer, and include information that will help the Commission monitor compliance with our third-party authentication rules. The agreement must specify the specific tasks that the third party will perform on the behalf of the provider with the STIR/SHAKEN implementation obligation, and confirm that the provider with the STIR/SHAKEN implementation obligation will: (1) make all attestation-level decisions for calls signed pursuant to the agreement, and (2) ensure that all calls will be signed using this provider's certificate. Providers may be required to submit a copy of the agreement to the Commission in connection with a review of the provider's compliance with these requirements or an investigation by the Enforcement Bureau. Under this rule, a current agreement must be in place for as long as any third-party authentication arrangement exists, and all copies of third-party agreements must be maintained for a period of two years from the end or termination of the agreement. The record reflects

that third-party authentication may particularly benefit small providers that may be burdened by the costs of deploying STIR/SHAKEN in the IP portion of their voice service network. The benefits of the third-party authentication rules adopted in the *Eighth Report and Order* will greatly exceed the minimal costs imposed on small providers.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to provide, "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."

The *Eighth Report and Order* considered alternatives that may minimize the economic impact on small providers. We authorize providers with a STIR/SHAKEN implementation obligation under the Commission's rules to engage in third-party authentication to comply with that obligation, subject to certain limitations. Our third-party authentication rules thus impose guardrails solely on those providers choosing to make use of a third party to comply with their obligation. Given evidence in the record that third-party authentication may help to reduce costs for small providers, we find that our explicit authorization of the practice, subject to certain guardrails, will enable those providers to accrue those benefits while remaining compliant with the Commission's STIR/SHAKEN implementation obligations. We also find that our action explicitly requiring all providers, regardless of whether they choose to engage in third-party authentication, to obtain an SPC token, use that token to obtain a certificate, and ensure that all calls are signed using that certificate, will be minimally burdensome for small providers, as evidenced by the record.

We also adopt an approach to authorizing third-party authentication that will ensure that our requirements do not unduly burden all providers, including small providers. Recognizing arguments in the record that providers could be required to make a number of commercial and network changes to comply with the newly adopted authentication requirements, we grant providers a minimum of 210 days following release of this *Report and Order* to comply with our rules. Finally, we also considered and decline to require providers to submit additional information to the Robocall Mitigation Database, which should thus reduce burdens on all providers.

G. Report to Congress

The Commission will send a copy of the *Eighth Report and Order*, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the *Eighth Report and Order*, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *Eighth Report and Order* (or summaries thereof) will also be published in the *Federal Register*.

III. PROCEDURAL MATTERS

Paperwork Reduction Act. This document may contain new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. All such new or modified information collection requirements will be submitted to the Office of Management and Budget (OMB) for review under the PRA. OMB, the general public, and other Federal agencies will be invited to comment on new or substantively modified information collection requirements contained in this proceeding. Any non-substantive modification to a previously approved information collection will be submitted to OMB for review pursuant to OMB's process for non-substantive changes. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission

might further reduce the information collection burden for small business concerns with fewer than 25 employees. In this present document, we have assessed the effects of: (1) requiring that any third-party authentication arrangement be memorialized in an agreement between the party with the STIR/SHAKEN implementation obligation under the Commission's rules and the third-party signer; and (2) allowing providers to certify to complete or partial implementation in the Robocall Mitigation Database *only* if they have obtained an SPC token and digital certificate and sign calls with their certificate. We find that small providers have had ample time to develop processes to allow them to respond within the appropriate time and that providers for which this presents a significant burden, either due to their size or for some other reason, may request a waiver. With respect to any non-substantive modification to a previously approved information collection, such changes are non-substantive and do not give rise to new or substantively modified information collection burdens for small business concerns with fewer than 25 employees pursuant to the Small Business Paperwork Relief Act of 2002.

Congressional Review Act. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is "major" under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this *Eighth Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

IV. ORDERING CLAUSES

Accordingly, pursuant to Sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 214, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503, IT IS ORDERED that this *Eighth Report and Order* IS ADOPTED.

IT IS FURTHER ORDERED that part 64 of the Commission's rules IS AMENDED as set forth in Appendix A.

IT IS FURTHER ORDERED that, pursuant to §§ 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR 1.4(b)(1), 1.103(a), this *Eighth Report and Order*, including the rule revisions and redesignations described in Appendix A, SHALL BE EFFECTIVE 30 days after its publication in the *Federal Register* following OMB approval. The Commission directs the Wireline Competition Bureau to announce the completion of any review by the Office of Management and Budget that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act and the relevant effective date by subsequent public notice.

IT IS FURTHER ORDERED that the Office of the Managing Director, Performance & Program Management, SHALL SEND a copy of this *Eighth Report and Order* in a report to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A).

IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Eighth Report and Order*, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 64

Carrier equipment, Communications common carriers, Reporting and recordkeeping requirements, Telecommunications, and Telephone.

Federal Communications Commission.

Marlene Dortch,

Secretary.

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR part 64 as follows:

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. The authority citation for part 64 continues to read as follows:

Authority: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 620, 716, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091; Pub. L. 117-338, 136 Stat. 6156.

Subpart HH—Caller ID Authentication

2. Amend § 64.6301 by revising paragraphs (a)(1) and (2) and adding paragraph (b) to read as follows:

§ 64.6301 Caller ID Authentication.

(a) * * *

(1) Obtain an SPC token from the Secure Telephone Identity Policy Administrator and use that token to obtain a Secure Telephone Identity certificate from a Secure Telephone Identity Certificate Authority;

(2) Using the certificate obtained pursuant to paragraph (a)(1) of this section:

(i) Authenticate and verify caller identification information for all SIP calls that exclusively transit its own network;

(ii) Authenticate caller identification information for all SIP calls it originates and that it will exchange with another voice service provider or intermediate provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path; and

* * * * *

(b) A voice service provider may fulfill its obligations to authenticate caller identification information under paragraph (a)(2) of this section by entering into an agreement with a third-party authentication service, provided that the voice service provider:

(1) Requires the third party to sign all calls using the certificate obtained by the voice service provider in accordance with paragraph (a)(1);

(2) Makes all attestation-level decisions regarding the caller identification information of each SIP call it originates;

(3) Memorializes the agreement between it and the third party for the authentication service in writing, which:

(i) Specifies the specific tasks that the third-party authenticator will perform on the voice service provider's behalf, and

(ii) Confirms that the voice service provider shall make all attestation-level decisions for calls signed pursuant to the agreement, and that all calls shall be signed using the voice service provider's Secure Telephone Identity certificate;

(4) Maintains any agreement entered into pursuant to paragraph (b) of this section for as long as any third-party authentication arrangement exists; and

(5) Retains a copy of any agreement entered into pursuant to paragraph (b) of this section for a period of two (2) years from the end or termination of the agreement.

3. Amend § 64.6302 by:

a. Redesignating paragraphs (a) through (d) as paragraph (b) through (e);

b. Adding new paragraphs (a) and (f); and

c. Revising newly redesignated paragraphs (c) introductory text, (d), and (e).

The additions and revisions read as follows:

§ 64.6302 Caller ID authentication by intermediate providers.

* * * * *

(a) Obtain an SPC token from the Secure Telephone Identity Policy Administrator and use that token to obtain a Secure Telephone Identity certificate from a Secure Telephone Identity Certificate Authority;

* * * * *

(c) Authenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call using the Secure Telephone Identity certificate it received from the Secure Telephone Identity Certificate Authority pursuant to paragraph (a) of this section, except that the intermediate provider is excused from such duty to authenticate if it:

* * * * *

(d) Notwithstanding paragraph (c) of this section, a gateway provider must authenticate caller identification information using the Secure Telephone Identity certificate it received pursuant to paragraph (a) of this section for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that gateway provider is subject to an applicable extension in § 64.6304.

(e) Notwithstanding paragraph (c) of this section, a non-gateway intermediate provider must authenticate caller identification information using the Secure Telephone Identity certificate it received pursuant to paragraph (a) of this section for all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that non-gateway intermediate provider is subject to an applicable extension in § 64.6304.

(f) An intermediate provider may fulfill its obligations to authenticate caller ID

information under paragraphs (d) and (e) of this section by entering into an agreement with a third-party authentication service, provided that the intermediate provider:

(1) Requires the third party to sign all calls using the certificate obtained by the intermediate provider in accordance with paragraph (a) of this section;

(2) Makes all attestation-level decisions regarding the caller identification information of each SIP call it originates;

(3) Memorializes the agreement between it and the third party for the authentication service in writing, which:

(i) Specifies the specific tasks that the third-party authenticator will perform on the intermediate provider's behalf, and

(ii) Confirms that the intermediate provider shall make all attestation-level decisions for calls signed pursuant to the agreement, and that all calls shall be signed using the voice service provider's Secure Telephone Identity certificate;

(4) Maintains any agreement entered into pursuant to paragraph (f) of this section for as long as any third-party authentication arrangement exists; and

(5) Retains a copy of any agreement entered into pursuant to paragraph (f) of this section for a period of two (2) years from the end or termination of the agreement.

4. Amend § 64.6303 by revising paragraphs (b)(1) and (c)(1) to read as follows:

§ 64.6303 Caller ID authentication in non-IP networks.

* * * * *

(b) * * *

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(d) throughout its network; or

* * * * *

(c) * * *

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(e) throughout its network; or

* * * * *

5. Amend § 64.6304 by revising paragraph (b) to read as follows:

§ 64.6304 Extension of implementation deadline.

* * * * *

(b) *Voice service providers, gateway providers, and non-gateway intermediate providers that cannot obtain an SPC token.* Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining an SPC token. Gateway providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(d) regarding call authentication. Non-gateway intermediate providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(e) regarding call authentication.

* * * * *

6. Amend § 64.6305 by revising paragraphs (d)(1)(i) and (ii), (e)(1)(i) and (ii), and (f)(1)(i) and (ii) to read as follows:

§ 64.6305 Robocall Mitigation and Certification.

* * * * *

(d) * * *

(1) * * *

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with § 64.6301;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion

of its network and all calls it originates on that portion of its network are compliant with § 64.6301(a) and (b); or

* * * * *

(e) * * *

(1) * * *

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302; or

* * * * *

(f) * * *

(1) * * *

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302; or

* * * * *

[FR Doc. 2025-15809 Filed: 8/18/2025 8:45 am; Publication Date: 8/19/2025]